UCRL- 82952
PREPRINT

THE MFTF EXCEPTION HANDLING SYSTEM

D. M. NOWELL
G. D. BRIDGEMAN

This paper was prepared for submittal to the
8th SYMPOSIUM ON ENGINEERING PROBLEMS OF
FUSION RESEARCH; IEEE; SHERATON HOTEL,
SAN FRANCISCO, CA., NOVEMBER 13-16, 1979

11-12-79

Lawrence
Livermore
Laboratory

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

THE MFTF EXCEPTION HANDLING SYSTEM*

D. M. Nowell, G. D. Bridgeman
Lawrence Livermore Laboratory
Livermore, California 94550

Summary

In the design of large experimental control systems, a major concern is ensuring that operators are quickly alerted to emergency or other exceptional conditions and that they are provided with sufficient information to respond adequately. This paper describes how the MFTF exception handling system satisfies these requirements. Conceptually exceptions are divided into one of two clases. Those which affect command status by producing an abort or suspend condition and those which fall into a softer notification category of report only or operator acknowledgement requirement. Additionally, an operator may choose to accept an exception condition as operational, or turn off monitoring for sensors determined to be malfunctioning. Control panels and displays used in operator response to exceptions are described.

Introduction

The remote control system for the Magnetic Fusion Test Facility (MFTF) will be responsible for monitoring and/or controlling all preparatory operations for experiment readiness, maintenance of an environment conducive to plasma shots, synchronization of events for shot firing, and preparatory operations for bringing the MFTF down for up-to-air maintenance. Nine subsystems are involved: External Vacuum Subsystem, Cryogenic Subsystem, Magnet Subsystem; Getter Subsystem; Safety Interlock Subsystem; Plasma Streaming Gun Subsystem, Start-up Neutral Beam Gun Subsystem, and Sustaining Neutral Beam Gun Subsystem.

A fundamental concern in the remote control operation of MFTF is ensuring that operators become quickly aware of emergencies; that they have sufficient details about the nature of the emergency to respond properly; and that they have adequate control to respond to exceptions so that they may return to their normal functions as quickly as possible. Meeting these needs represent the major goals of the MFTF exception handling system. Either augmenting or incorporating these goals are the following design specifications for the exception system: detect exceptions and report them to the operator; provide an audit trail of exception occurrences for operator event analysis and safety review; serve as a backup to the hard-wired subsystem protection systems; help the operator detect abnormal operational trends so he can take corrective action before more drastic hard-wired action is taken; and aid the operator in identifying malfunctioning sensors.

Exceptions are defined as deviations from normal operating conditions. Exception types are as follows:

- A change in state of a monitored value. (Most measurement-monitored parameters have one or more of the following five range states: high critical, high alarm, normal, low alarm, and low critical. Any range change will be reported as an exception, hence a return to normal value will also be reported.)
- A change in a status signal. (These are generally alarm signals tied into hardware monitoring systems.)
- A degradation in the performance of certain operations. (An example of this type of exception is failure to meet a set point within a required time limit.)

Depending upon the nature of the exception and the time criticality of response action, responses to exceptions fall into three main categories:

- Hardwired response of which the remote control system is made aware and which require no computer intervention.

  Preprogrammed software action taken immediately by the remote control system.

- Responses selected by an operator seeking to take corrective action.

The MFTF exception system is designed to present the operator with only valid and useful data, and to provide some aid in selecting a proper response to an exception. The main subject of this paper is therefore, the operator's view of the MFTF exception handling system.

MFTF operators work at remote consoles fitted with three or six display CRTs for status viewing and two touch-sensitive panels for command entry. A selection of displays and control panel pictures are available to the operator from which he selects, for display, those pertinent to current control functions. Large hard panels displaying status information are not a part of the remote control system. Each console has a functional assignment of the subsystems that may be controlled from it, and some consoles have more subsystem control than others. Operators controlling a particular subsystem must be logged into an appropriate console and must have claimed ownership for that subsystem. New exceptions that occur within a subsystem are signalled by a message that appears on the lower portion of the center display CRT of the console where current ownership resides. Algorithms exist for rerouting an exception message if there is no current owner for the subsystem. Additionally, operators may request to view exception messages for subsystems they do not currently own, and exception messages will be directed to them also.

The exception attention message displays the following information:

Countdown held or aborted (if appropriate)

N exceptions waiting to be listed	Brief description of the highest priority exception yet to be listed

*Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore Laboratory under contract number W-7405-ENG-48.

It is banded by two blinking lines that are color-coded to reflect the highest priority within the wait list: light blue for return to normal, yellow to reflect an alarm condition; red to reflect a critical condition. If the exception condition involves a high degree of danger to personnel or the MFTF itself, an audible alarm is used to supplement the visual message as an attention-getter.

Located on the bottom lines of each touch panel are two control buttons outlined in red to easily identify their exception-processing association. These buttons are always available, independent of the current control panels selected. They are:

LIST EXCEP	PROC EXCEP

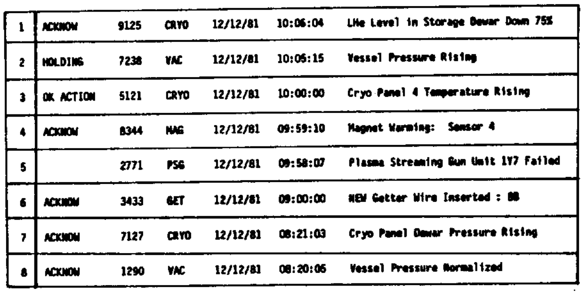
When the attention message flashes to alert the operator of new exceptions, the operator should press:

LIST
EXCEP

This automatically displays a report list describing the new exception arrivals. Specifically, the following actions are performed. The N exceptions waiting to be listed are added to the exception report display if it is currently being displayed. If not, the report is formed and automatically displayed on the console's left CRT. If N exceptions cannot be displayed because of screen size, then the oldest 22 exceptions yet to be reported will be displayed and the center message will indicte that N-22 exceptions are waiting to be reported. When no additional exception messages are waiting to be listed, the attention message disappears.

Because the CRT screen size limits the number of exceptions that can be viewed at one time, and the control system only buffers a finite number of exception messages, a dedicated line printer logs exceptions as they occur to provide a hard-copy record of exception events. Additionally, at exception detection time, a description of the exception and its time of occurrence is logged to a journal file. The journal file is written to tape as a permanent record.

The exception report display is the key display for the exception system. An example of a report display is shown in Fig. 1. The top half of the display contains the most recent exceptions, and the bottom half can be scrolled to view a maximum of 75 exceptions. Messages are dropped from the exception report via ageing, regardless of any action taken; the oldest messages are the first to be dropped when new messages arrive, if sufficient buffer space is not available.



1	ACKNOW	9125	CRYO	12/12/81	10:06:04	LHe Level in Storage Dewar Down 75%
2	HOLDING	7238	VAC	12/12/81	10:06:15	Vessel Pressure Rising
3	OK ACTION	5121	CRYO	12/12/81	10:00:00	Cryo Panel 4 Temperature Rising
4	ACKNOW	8344	MAG	12/12/81	09:59:10	Magnet Warming: Sensor 4
5		2771	PSG	12/12/81	09:58:07	Plasma Streaming Gun Unit 1Y7 Failed
6	ACKNOW	3433	GET	12/12/81	09:00:00	NEW Getter Wire Inserted : 88
7	ACKNOW	7127	CRYO	12/12/81	08:21:03	Cryo Panel Dewar Pressure Rising
8	ACKNOW	1290	VAC	12/12/81	08:20:06	Vessel Pressure Normalized

Fig. 1

Exception Handling Display

Each exception message in the report contains the following information:

Response Field

A response field is displayed that dictates the type of operator response for the exception: OK ACTION; ACKNOW; HOLDING. The operator must verify computer-selected action, acknowledge the exception, and either abort or continue the operation holding. The field is color-coded where red, yellow, and light-blue signify critical, alarm, and normal status, respectively. The field blinks to serve as a "nuisance" to force the operator to take action, and as a reminder that response action is still pending for this exception. The appropriate action on the PROCESS EXCEPTIONS panel will terminate blinking. If the exception is of the report only type this field remains blank.

Audible Indicator

A special character is displayed to the left of an exception report to indicate if the exception has triggered an audible alarm.

Exception Number

The exception number is displayed (Each exception has a unique number.) This number is color-coded the same as the response field.

Primary Subsystem

The primary subsystem involved is indicated and color-coded to match the response field and exception number.

Time of Occurance

The date and time of occurance is displayed in white.

Exception Description

Approximately 40 characters remain for a short description of the exception, which can present a problem for complicated exceptions. The EXPANDED EXCEPTION DESCRIPTION display helps to alleviate this problem. Until the operator responds to an exception as specified in the response field, the background of the date and description fields is dark blue (instead of black) as a reminder that response action has not been taken for this exception. For report only messages, the background is dark blue until the display is updated.

Return to Normal Check

Exceptions that have cleared are tagged by a light blue check made at the left edge of the exception report message to indicate that the exception condition has now returned to a normal state.

To summarize, the exception report provides a brief description of the exception and specifies what operator response action is required.

All control functions keyed to these response actions have been grouped on a single PROCESS EXCEPTIONS control panel. Several control panels are associated with exception handling, but virtually all exception processing can be handled with the PROCESS EXCEPTIONS panel. This panel is brought up by pressing the button

PROC
EXCEP

located on the bottom line of all control panels. The control panel is shown in Fig. 2. Almost all control function buttons require that an operator identify the exception to which the function will be applied.

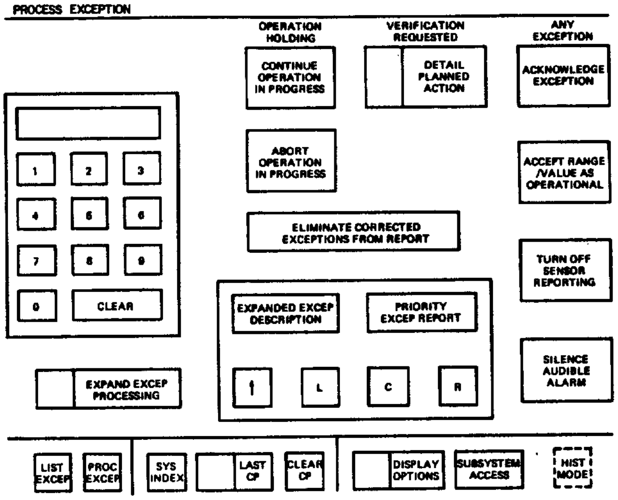


Fig. 2

To do this, the operator "keys in" either the exception's unique identification number or the line number of the exception, followed by the desired control response. The exception control responses are listed below:

- Acknowledge Exception
- Abort Operation in Progress
- Continue Operation in Progress
- Detail Planned Action
- Accept Range/Value as Operational
- Turn Off Exception Reporting
- Silence Audible Alarm
- Expand Exception Description
- Priority Exception Report
- Eliminate Corrected Exception From Reports
- Expanded Exception Processing

Acknowledge Exception

This indicates only that the operator has acknowledged the exception.

Abort Operation In Progress

The specified command currently in a HOLD state as a consequence of the exception occurrence is aborted.

Continue Operation in Progress

The specified command currently in a HOLD state as a consequence of the exception occurrence is permitted to continue.

Detail Planned Action

By selecting this control function the operator causes another control panel to be "brought up" to give the operator hints about corrective action to take or critical parameters to watch. The format of the panel varies with the exception, performing the possible functions listed:

- This panel may list actions selected by the subsystem that could alleviate the condition causing the exception. The operator can select which actions to confirm, or--by just pressing ENABLE VERIFICATION--all functions are performed in the order listed. No verification is desired, ENABLE CANCEL ACTIONS are pushed. Some operations may degrade if the operator cancels planned actions. However, the operator retains primary responsibility for his or her actions.

- This panel may provide easy access to control panels needed to take care or the exception. In this way, the operator need not remember how to call up the indicated panels.

- This panel may simply provide information on which sensors to watch. This would be the case when no definitive course of action can be determined and the necessary control panels cannot be adequately defined.

Accept Range/Value As Operational

The range in which the exception occurred is temporarily extended as being normal or operational. If the exception value lies in the critical range, the new normal range will only include that particular value, not the entire range; values occurring within declared accepted ranges do not trigger exception reports. The accepted ranges remain in effect until cancelled by an operator. When a sensor for which the normal range has been extended is displayed, the value display is colored to represent the new exception range. A "*" character colored to represent the original exception status is prefixed to all displayed values from such monitors.

Turn Off Exception (Sensor) Reporting

The operator has the capability of turning off exception reporting of sensors considered to be malfunctioning. This is to prevent the sensor from causing annoying exception messages. Sensors whose exception report capability have been turned off are logged as requiring maintenance. The operator can only turn a sensor on again from a maintenance control panel. Monitored values of sensors turned off are preceded by a "?" on displays to remind the operator that the sensor's output is questionable.

Expanded Exception Description

This function is used to expand on the brief description provided in the exception report. The expanded description is formatted as a display and varies with individual exceptions. The display is used to present any information that might be helpful to the operator, either regarding the particular exception in general or how that exception relates presently to other system inputs. This display can be text but it is preferably pictorial in nature.

Priority Exception Report

This report, formatted as a display, allows the operator to view exception messages ordered by their criticality.

Expanded Exception Processing

Selecting this control function will bring up the control panel shown in Fig. 3. For the purposes of this paper, the control functions themselves are sufficient to indicate the types of expanded exception processing supported by the system.

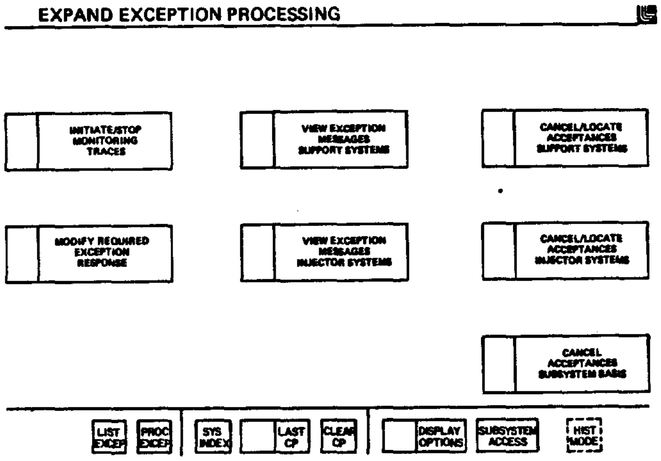

EXPAND EXCEPTION PROCESSING
INITIATE/STOP MONITORING TRACES
VIEW EXCEPTION MESSAGES SUPPORT SYSTEMS
CANCEL/LOCATE ACCEPTANCES SUPPORT SYSTEMS
MODIFY REQUIRED EXCEPTION RESPONSE
VIEW EXCEPTION MESSAGES INJECTOR SYSTEMS
CANCEL/LOCATE ACCEPTANCES INJECTOR SYSTEMS
CANCEL ACCEPTANCES SUBSYSTEM BASIS
LIST EXCEP
PROC EXCEP
SYS INDEX
LAST CP
CLEAR CP
DISPLAY OPTIONS
SUBSYSTEM ACCESS
HIST MODE

Fig. 3

Conclusion

The operator's view of the MFTF exception handling system is described. The system design overcomes such traditional alarm system problems as lack of a permanent record, inflexibility, and operator confusion. Exception messages contain only valid, useful data. Consolidation of exception reports via combinatorial analysis is provided at the individual subsystem level and a global level. Criticality of exceptions is easily recognized by consistent color-coding to aid operators in determining the priority of response actions. Displays and control panels are available to help operators respond quickly in selecting corrective action to take.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately-owned rights.

Reference to a company or product name does not imply approval or recommendation of the product by the University of California or the U.S. Department of Energy to the exclusion of others that may be suitable.